INFORMATION AND CONTROL 28, 292–303 (1975)

Upper Bounds on the Cardinality of a Binary Code with a Given Minimum Distance*

V. M. SIDELNIKOV

Communicated by E. R. Berlekamp

This paper obtains an upper bound on the cardinality of a binary code of length n and minimum distance d, which improves on the Elias bound exponentially in n. A new upper bound for the cardinality of a constant-weight binary code is also presented.

1. INTRODUCTION

This paper presents in detail results which were announced in Sidelnikov (1973).

Let $d = d(n)$, $r = r(n)$ be integer-valued functions of n such that $\lim_{n\to\infty} d/n = \delta$, $0 < \delta \leqslant 1/2$ and $\lim_{n\to\infty} r/n = \rho$, $0 < \rho < 1$. Let $m(n, d)$ be the maximal cardinality of a binary code of length n with minimum distance d, and $m_r(n, d)$ the maximal cardinality of a binary code with minimum distance d, all of whose codewords have weight r. This paper obtains the following estimates:

$$n^{-1} \ln m(n, d) \lesssim \ln 2 - H(1/2 - (1 - 2\delta)^{1/2}/2) - \epsilon(\delta), \qquad n \to \infty, \quad (1)$$

where $H(x) = -x \ln x - (1 - x) \ln(1 - x)$ and $\epsilon(\delta)$ is a certain function[1] of δ such that $\epsilon(\delta) > 0$ for $0 < \delta < 1/2$, and

$$n^{-1} \ln m_r(n, d) \lesssim (\alpha - g) \ln((g - \alpha + \alpha^2)/\alpha^2) \ln(1 - \delta(2g)^{-1}), \qquad n \to \infty, \quad (2)$$

* The original paper appeared in *Probl. Peredachi Inform.* 10, 2 (1974), 43–51. Translation by A. M. Odlyzko, Bell Laboratories, Murray Hill, NJ 07974.

[1] The right side of (1) represents a function (presented explicitly in Section 3) whose arguments are δ and the solutions (x_0, y_0) to a system of transcendental equations depending on δ.

where[2] $g = \rho(1 - \rho)$, $0 < \delta/2 \leqslant g$ and α, $0 < \alpha \leqslant g$ is the root of

$$\delta/2 = g - (g - \alpha) \exp \frac{\rho H(\alpha/\rho) + (1 - \rho) H(\alpha/(1 - \rho)) - H(\rho)}{(g - \alpha) \ln((g - \alpha + \alpha^2)/\alpha^2)}. \quad (3)$$

The estimate (1) improves on the well-known Elias bound (cf., Berlekamp, 1971; Bassalygo, 1965): $n^{-1} \ln m(n, d) \lesssim \ln 2 - H(1/2 - (1 - 2\delta)^{1/2}/2)$, $n \to \infty$, while estimate (2) for large n and for $\delta(\delta < 2g)$ belonging to a certain neighborhood of $2g$ improves on the corresponding estimate of Levenshtein (1971). It should also be mentioned that in 1971 the author published an estimate (Theorem 2 of Sidelnikov, 1971) of the form $d(n, m, q) \leqslant \phi(n, m, q)$, where $d(n, m, q)$ is the maximum of the minimal distances of q-ary codes ($q \geqslant 2$) of length n, which contain m codewords. If we represent this estimate in the form

$$n^{-1} \ln m(n, d, r) \lesssim \Psi(\delta, q), \qquad n \to \infty, \quad (4)$$

[$m(n, d, r)$ = maximal cardinality of a q-ary code of length n with minimum distance d], then it improves exponentially in n on the corresponding Elias bound, provided δ belongs to an interval $(\delta_0, (q - 1)/q)$, where $\delta_0 = \delta_0(q)$ is a certain constant less than $(q - 1)/q$. In particular, for $q = 2$ the estimate (4) is of the form (1) for $\delta \in (\delta_0, 1/2)$. The estimate (1) improves and extends this result in the case $q = 2$.

Let us now outline the proofs of (1) and (2).

It is known (Bassalygo, 1965) that

$$m(n, d) \leqslant 2^n m_r(n, d)/C_n^r. \quad (5)$$

If we estimate $m_r(r, d)$ in (5) with the help of (2) and then find the minimum with respect to r of the resulting expansion, we will obtain the estimate (1). Thus the main difficulty of this paper is in the derivation of (2).

Let us denote by E_n^r the set of all binary vectors of weight r. In the vectors of E_n^r let us replace 1's by the real number $-((n - r)/(nr))^{1/2}$, and 0's by $(r/(n(n - r)))^{1/2}$. This replacement defines a one-to-one transformation $\mathfrak{A}$ of the set E_n^r into the set $\mathscr{E}_n^r$, consisting of vectors having r coordinates equal to $-((n - r)/(nr))^{1/2}$ and $n - r$ coordinates equal to $(r/(n(n - r)))^{1/2}$. It is clear that $\mathscr{E}_n^r$ lies[3] on the surface of the $(n - 1)$-dimensional sphere S_n of radius 1 in the Euclidean space R^n.

[2] For $\delta/2 = g$ the right side of (2) is to be regarded as 0.

[3] In fact $\mathscr{E}_n^r$ belongs even to S_{n-1}, since the sum of the coordinates of the points in $\mathscr{E}_n^r$ equals 0.

Let $\lambda(\mathbf{x}, \mathbf{y})$, $\mathbf{x}, \mathbf{y} \in R^n$ denote the usual Euclidean metric and for any finite subset $\mathscr{K}$ of S_n let $\lambda(\mathscr{K}) = \min_{\mathbf{x},\mathbf{y}\in\mathscr{K},\mathbf{x}\neq\mathbf{y}} \lambda(\mathbf{x}, \mathbf{y})$. Then $\mathfrak{A}$ transforms the set E_n^r with the Hamming metric $d(\mathbf{a}, \mathbf{b})$, $\mathbf{a}, \mathbf{b} \in E_n^r$ into the set $\mathscr{E}_n^r$, which has the Euclidean metric $\lambda(\mathbf{x}, \mathbf{y})$. It is obvious that these metrics are related by $\lambda(\mathfrak{A}a, \mathfrak{A}b) = (nd(\mathbf{a}, \mathbf{b})/(r(n-r)))^{1/2}$. Therefore

$$\lambda(\mathfrak{A}(K)) = (nd(K)/(r(n-r)))^{1/2}, \tag{6}$$

where K is any subset (code) of E_n^r, $d(K)$ the minimum distance of K, and $\mathfrak{A}(K)$ the image of K under $\mathfrak{A}$.

Let us call any finite set $\mathscr{K} \subset S_n$ a λ-set if $\lambda(\mathscr{K}) \geqslant \lambda$. The indicated relationship between metric properties of E_n^r and $\mathscr{E}_n^r$ shows that $m_r(n, d)$ equals the maximum cardinality of a $(nd/(r(n-r)))^{1/2}$-set, whose points belong to $\mathscr{E}_n^r$.

Upper estimates for the number of points of an arbitrary λ-set were obtained in Sidelnikov (in print). If we were to use those estimates to estimate $m_r(n, d)$, then with their help and (5) we could (for suitable r) deduce an estimate of the form (1). However, in such a proof of (1) we would not be utilizing the fact that elements of the set $\mathfrak{A}(K)$ are not distributed arbitrarily in S_n, but have to be contained among the elements of $\mathscr{E}_n^r$. Making use of this property, we will obtain below estimates of $m_r(n, d)$ which are slightly stronger than those which follow directly from the results of Sidelnikov (in print).

To obtain estimates of $m_r(n, d)$ we will consider in this paper, just as in Sidelnikov (in press), the sums

$$M_t(\mathscr{K}) = \sum_{\mathbf{x}\in\mathscr{K}} \sum_{\mathbf{y}\in\mathscr{K}} (\mathbf{x}, \mathbf{y})^t,$$

where $\mathscr{K}$ is a subset of $\mathscr{E}_n^r$ containing m elements. (In Sidelnikov, in press' $\mathscr{K}$ is any subset of S_n.) It turns out that one can show (Corollary 1) that for any $\mathscr{K}$, $\mathscr{K} \subset \mathscr{E}_n^r$,

$$M_t(\mathscr{K}) \geqslant m^2\sigma(n, t), \tag{7}$$

where $\sigma(n, t)$ is an explicitly specified constant, depending only on n and t. This result[4] is a corollary of a general inequality (v. Lemma 1) connected with the distribution of points in R^n which lie on surfaces satisfying certain homogeneous equations.

[4] An analogous result holds for an arbitrary set $\mathscr{K}$, $\mathscr{K} \subset S_n$, with a constant $\sigma'(n, t)$ which is smaller than $\sigma(n, t)$ (cf. Sidelnikov, in print).

Let us note further that $\lambda^2(\mathbf{x}, \mathbf{y}) = 2(1 - (\mathbf{x}, \mathbf{y}))$ if $\mathbf{x}, \mathbf{y} \in S_n$, where $(\mathbf{x}, \mathbf{y})$ is the inner product in R^n. Thus

$$\lambda^2(\mathscr{K}) = 2(1 - \gamma(\mathscr{K})), \tag{8}$$

where $\gamma(\mathscr{K}) = \max_{\mathbf{x},\mathbf{y}\in\mathscr{K},\mathbf{x}\neq\mathbf{y}} (\mathbf{x}, \mathbf{y})$. Therefore an upper bound for $\lambda(\mathfrak{A}(K))$ is equivalent to a lower bound for $\gamma(\mathfrak{A}(K))$. Lower bounds for $\gamma(\mathfrak{A}(K))$ are easy to obtain (v. Theorem 1) with the help of inequality (7). To deduce (2) it then only remains to "invert" (v. Theorem 2) the resulting bound; i.e., from an estimate of the form $\lambda = \lambda(\mathfrak{A}(K)) \leqslant \phi(m, n)$ to deduce a bound of the form $m \leqslant \psi(\lambda, n)$.

2. Bound on the Cardinality of a Constant-Weight Binary Code

We will use the following notation: k, h, n, t, s, u, and i, j, l with subscripts will denote positive integers; $\sigma_t(\mathbf{x}) = \sum_{k=1}^{n} x_k{}^t$, where $\mathbf{x} = (x_i, \ldots, x_n) \in R^n$; $S_n(\nu_1, \nu_2, \ldots, \nu_t)$ a subset of R^n, consisting of elements satisfying $\sigma_u(\mathbf{x}) = \nu_u$, $u = 1, \ldots, t$; $\sum^{*}_{l_1+\ldots+l_h=t}$ a sum over all ordered n-tuples of positive integers $(l_1, \ldots, l_h)$ for which $l_1 + \cdots + l_h = t$; $\sum'_{(j_1,\ldots,j_h)}$ a sum over all ordered n-tuples of integers $(j_1, \ldots, j_h)$, $1 \leqslant j_k \leqslant n$, $k = 1, \ldots, h$, with $j_k \neq j_l$ for $k \neq l$.

The following lemma is presented in a much more general form than will be used later. If desired, the reader can regard the integrals appearing in this lemma as the corresponding sums which appear in the proof of Corollary 1.

Lemma 1. *Let U and U' be subsets of a nonempty set $S_n(\nu_1, \ldots, \nu_t)$, $t \geqslant 1$, and let μ and μ' be measures defined on U and U', respectively, such that*

$$\int_U \mu(d\mathbf{x}) = \int_{U'} \mu'(d\mathbf{x}) = 1 \tag{9}$$

and if $t = 1$

$$\int_U |x_i| \, \mu(d\mathbf{x}) < \infty, \qquad \int_{U'} |x_i| \, \mu'(d\mathbf{x}) < \infty, \qquad i = 1, \ldots, n,$$

where $\mathbf{x} = (x_1, \ldots, x_n)$.

Suppose that the measure μ' has the following property:

(a) *For any fixed n-tuple of positive integers $(l_1, \ldots, l_h)$, $1 \leqslant h \leqslant t$, $l_1 + \cdots + l_h = t$, the value of the integral*

$$\int_{U'} x_{j_1}^{l_1} \cdots x_{j_h}^{l_h} \mu'(d\mathbf{x})$$

is the same for all n-tuples $(j_1,\ldots,j_h)$, $1 \leqslant j_k \leqslant n$, $k = 1,\ldots,h$, *with pairwise distinct entries.*

Then

$$\int_U \int_U (\mathbf{x},\mathbf{y})^t \mu(d\mathbf{x})\,\mu(d\mathbf{y}) \geqslant \int_{U'} \int_{U'} (\mathbf{x},\mathbf{y})^t \mu'(d\mathbf{x})\,\mu'(d\mathbf{y}). \tag{10}$$

Equality holds if and only if μ *satisfies property* (a).

Proof. Let M_t and M_t' denote the left and right sides of (10). From the obvious bound $|x_j| \leqslant \nu_2^{1/2}$, $j = 1,\ldots,n$, valid for $t > 1$, and from the condition of the lemma we obtain

$$\int_U |x_{i_1} \cdots x_{i_t}|\,\mu(d\mathbf{x}) < \infty.$$

Therefore

$$M_t = \int_U \int_U \sum_{(i_1,\ldots,i_t)} x_{i_1} \cdots x_{i_t} y_{i_1} \cdots y_{i_t} \mu(d\mathbf{x})\,\mu(d\mathbf{y})$$

$$= \sum_{(i_1,\ldots,i_t)} \left(\int_U x_{i_1} \cdots x_{i_t} \mu(d\mathbf{x})\right)^2. \tag{11}$$

Let us denote by I the set of integer all t-tuples $\mathbf{a} = (i_1,\ldots,i_t)$, $1 \leqslant i_k \leqslant n$, $k = 1,\ldots,t$; by I_h, the subset of I, consisting of all t-tuples $\mathbf{a}$, formed by h distinct integers; by $I(j_1,\ldots,j_h)$, the subset of I_h consisting of t-tuples $\mathbf{a}$, formed by the pairwise distinct integers $j_1,\ldots,j_h$, and, finally, by $I_{j_1\cdots j_h}^{l_1\cdots l_h}$, where $j_1,\ldots,j_h$ are pairwise distinct integers and $(l_1,\ldots,l_h)$ an h-tuple of positive integers with $l_1 + \cdots + l_h = t$, the subset of $I(j_1,\ldots,j_h)$ consisting of t-tuples $\mathbf{a}$, formed by the integers j_k, $k = 1,\ldots,h$, where each j_k appears in $\mathbf{a}$ l_k times.

Because of their construction the sets $I_{j_1\cdots j_h}^{l_1\cdots l_h}$ possess the following properties.

1. Two sets $I_{j_1\cdots j_h}^{l_1\cdots l_h}$ and $I_{j_1'\cdots j_h'}^{l_1'\cdots l_h'}$ coincide if the first symbol can be obtained from the second by a simultaneous permutation of upper and lower indices, and do not intersect otherwise.

2. From Property 1 it follows that each t-tuple $\mathbf{a} \in I_h$ belongs to $h!$ sets $I_{j_1\cdots j_h}^{l_1\cdots l_h}$.

3. The number of elements of $I_{j_1\cdots j_h}^{l_1\cdots l_h}$ is $(t!)/(l_1! \cdots l_h!)$.

4. Because of the commutativity of real number multiplication, the integral $\int_U x_{i_1} \cdots x_{i_t} \mu(d\mathbf{x})$ has the same value for all $(i_1,\ldots,i_t) \in I_{j_1\cdots j_h}^{l_1\cdots l_h}$.

From these properties and (11) it follows that

$$M_t = \sum_{h=1}^{t} (h!)^{-1} \sum_{l_1+\cdots+l_h=t}^{*} \sum_{(j_1,\ldots,j_h)}' \sum_{I_{j_1\cdots j_h}^{l_1\cdots l_h}} \left(\int_U x_{i_1} \cdots x_{i_t} \mu(d\mathbf{x})\right)^2$$

$$= \sum_{h=1}^{t} \sum_{l_1+\cdots+l_h=t}^{*} \frac{t!}{l_1! \cdots l_h! h!} \sum_{(j_1,\ldots,j_h)}' \left(\int_U x_{j_1}^{l_1} \cdots x_{j_h}^{l_h} \mu(d\mathbf{x})\right)^2.$$

Let us bound the last sum with the help of the Cauchy–Bunyakovsky inequality

$$\sum_{i=1}^{T} a_i^2 \geqslant T^{-1} \left(\sum_{i=1}^{T} a_i\right)^2,$$

where we put $a_i = \int_U x_{j_1}^{l_1} \cdots x_{j_h}^{l_h} \mu(d\mathbf{x})$. As a result we obtain

$$M_t \geqslant \sum_{h=1}^{t} \sum_{l_1+\cdots+l_h=t}^{*} \frac{t!}{l_1! \cdots l_h! h! A_n^{\,h}} \left(\int_U \sum_{(j_1,\ldots,j_h)}' x_{j_1}^{l_1} \cdots x_{j_h}^{l_h} \mu(d\mathbf{x})\right)^2, \quad (12)$$

where $A_n^{\,h} = n(n-1)\cdots(n-h+1)$ is the number of summands in $\sum_{(j_1,\ldots,j_h)}'$.

The sum $\Phi(\mathbf{x}) = \sum_{(j_1,\ldots,j_h)}' x_{j_1}^{l_1} \cdots x_{j_h}^{l_h}$ represents a symmetric function of degree t in the coordinates of the vector $\mathbf{x} = (x_1, \ldots, x_n)$ and, therefore, may be expressed in terms of the functions $\sigma_u(\mathbf{x})$, $u = 1, \ldots, t$. Hence for any $\mathbf{x} \in U \subset S_n(\nu_1, \ldots, \nu_t)$ the value of $\Phi(\mathbf{x})$ does not depend on $\mathbf{x}$ and equals a certain constant $C_{l_1\ldots l_h}(\nu_1, \ldots, \nu_t)$. From this, (9), and (12) it follows that

$$M_t \geqslant \sum_{h=1}^{t} \sum_{l_1+\cdots+l_h=t}^{*} \frac{t!}{l_1! \cdots l_h! h! A_n^{\,h}} C_{l_1\ldots l_h}^2(\nu_1, \ldots, \nu_t). \quad (13)$$

Let us now show that the right side of (13) equals M_t'. For this purpose we consider inequality (12) with μ' and U' in place of μ and U. In view of condition (a) of the lemma, this inequality becomes an equality and its right side equals the right side of (13), which proves the validity of (10).

From the conditions for equality in the Cauchy–Bunyakovsky inequality it immediately follows that equality holds in (12) if and only if μ satisfies condition (a). This proves the lemma.

Let us define

$$R_t(n, r) = (C_n^{\,r})^{-1} \sum_{j=0}^{n} C_r^{\,j} C_{n-r}^{j} \left(1 - \frac{jn}{(r(n-r))}\right)^t. \quad (14)$$

COROLLARY 1. *Let $\mathscr{K}$ be a subset of $\mathscr{E}_n^r$ (cf. Section 1), containing m elements. Then*[5]

$$1/m^2 \sum_{\mathbf{x}\in\mathscr{K}} \sum_{\mathbf{y}\in\mathscr{K}} (\mathbf{x}, \mathbf{y})^t \geqslant R_t(n, r). \tag{15}$$

Proof. Obviously, $\mathscr{E}_n^r$ is contained in the set $S_n(\nu_1, \ldots, \nu_t)$, where $\nu_k = (-1)^h r((n-r)/(rn))^{k/2} + (n-r)(r/((n-r)n))^{k/2}$, $k = 1, \ldots, t$. In Lemma 1 let us put $U = \mathscr{K}$, $\mu(\mathbf{x}) = m^{-1}$, $\mathbf{x} \in \mathscr{K}$; $U' = \mathscr{E}_n^r$, $\mu'(\mathbf{x}) = (C_n^r)^{-1}$, $\mathbf{x} \in \mathscr{E}_n^r$ (C_n^r is the number of elements of $\mathscr{E}_n^r$).

In this case the integrals $\int_U$ and $\int_{U'}$ represent the sums $m^{-1}\sum_{\mathbf{x}\in\mathscr{K}}$ and $(C_n^r)^{-1}\sum_{\mathbf{x}\in\mathscr{E}_n^r}$ so that the left side of (10) equals the left side of (15), and the right side of (10) equals $(C_n^r)^{-2}\sum_{\mathbf{x},\mathbf{y}\in\mathscr{E}_n^r}(x, y)^t$, which, as is easily shown, equals the right side of (14). Condition (a) of Lemma 1 is satisfied for $\sum_{\mathbf{x}\in\mathscr{E}_n^r}$, since all the elements of $\mathscr{E}_n^r$ are generated from a single one through all possible coordinate permutations. This proves the corollary.

COROLLARY 2. $R_t(n, r) \geqslant 0$ *for* odd t.

Proof. In Eq. (11) put $U = U'$, $\mu = \mu'$, where U' and μ' are defined as in the proof of Corollary 1. As a result we obtain an identity in which the left side equals $R_t(n, r)$, and the right side is a sum of nonnegative quantities.

Remark 1. The function $R_t(n, r)$ can be represented in the following form, which is convenient for calculation when t is not too large:

$$R_t(n, r) = (C_n^r)^{-1} \sum_{p=0}^{t} (-1)^p C_t^p (n/(r(n-r)))^p \sum_{k=0}^{p} C_{n-k}^r S(p, k)(r)_k, \tag{16}$$

where $(x)_k = x(x-1)\cdots(x-k+1)$ and $S(p, k)$ is a Stirling number of the second kind.

Proof. It follows from the relations $(j)_k C_r^j = (r)_k C_{r-k}^{j-k}$ and $\sum_{j=0}^{n} C_{r-k}^{j-k} C_{n-r}^j = C_{n-k}^r$ that

$$\sum_{j=0}^{n} (j)_k C_r^j C_{n-r}^j = (r)_k C_{n-k}^r. \tag{17}$$

In Eq. (14) let us expand $1 - jn(r(n-r))^{-1}$ raised to the power t by the binomial theorem, replace j^p in the resulting double sum by $\sum_{k=0} S(p, k)(j)_k$, change the order of summation and utilize (17). As a result we obtain (16).

[5] The right side of (15) can also be written in the form $M(\eta_1, \eta_2)^t$, where η_1, η_2 are independent random (vector) variables, distributed uniformly on $\mathscr{E}_n^r$, and M denotes mathematical expectation.

Using (16), we obtain the following expressions for $R_t(n, r)$:

$$R_1(n, r) = 0, \quad R_2(n, r) = 1/(n-1), \quad R_3(n, r) = \frac{n^2 - 4r(n-r)}{r(n-r)(n-1)(n-2)},$$
$$n > r > 0, \quad n > 2.$$

THEOREM 1. *Let* $\sigma_r(t, n, m) = (m-1)^{-1}(mR_t(n, r) - 1)$, $r \leqslant n/2$, *and let* s *be any positive integer for which the following two relations are satisfied*[6]:

$$\sigma_r(2s, n, m) > 0,$$
$$\Phi_r(s, n, m) = (\sigma_r(2s, n, m))^{(2s+1)/(2s)} + \sigma_r(2s+1, n, m) > 0.$$

Then

$$d_r(n, m) \leqslant 2r(n-r)(1 - (\tfrac{1}{2}\Phi_r(s, n, m))^{1/(2s+1)})/n, \tag{18}$$

where $d_r(n, m)$ *is the maximal minimum distance of a binary code of length* n, *consisting of* m *codewords of weight* r.

Proof. Let K be a binary code of length n, consisting of m codewords of weight r, and let $\mathfrak{A}(K)$ be the image of K under the transformation $\mathfrak{A}$ (cf. Section 1). In view of (6) and (8), to prove the theorem it suffices to show

$$\gamma(\mathfrak{A}(K)) \geqslant (\tfrac{1}{2}\Phi_r(s, n, m))^{1/(2s+1)}.$$

Let us denote by ξ_i, $i = 1, \ldots, m_1$, the numbers $(\mathbf{x}, \mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathfrak{A}(K)$, $\mathbf{x} \neq \mathbf{y}$, which are greater than 0, and by ζ_j, $j = 1, \ldots, m_2$ the absolute values of those numbers $(\mathbf{x}, \mathbf{y})$, $\mathbf{x}, \mathbf{y} \in \mathfrak{A}(K)$ which are less than 0. Clearly, $m_1 + m_2 \leqslant m(m-1)$.

From Corollary 1 we obtain

$$\sum_{\substack{\mathbf{x}, \mathbf{y} \in \mathfrak{A}(K) \\ \mathbf{x} \neq \mathbf{y}}} (\mathbf{x}, \mathbf{y})^t = \sum_{i=1}^{m_1} \xi_i{}^t + (-1)^t \sum_{j=1}^{m_2} \zeta_j{}^t \geqslant m^2 R_t(n, r) - m. \tag{19}$$

From Hölder's inequality (Hardy, Littlewood, and Polya, 1948, p. 39) and (19) we obtain

$$\sum_{i=1}^{m_1} \xi_j^{2s+1} + \sum_{j=1}^{m_2} \zeta_j^{2s+1} \geqslant (m(m-1))^{-1/(2s)} \times \left(\sum_{i=1}^{m_1} \xi_i^{2s} + \sum_{j=1}^{m_2} \zeta_j^{2s} \right)^{(2s+1)/(2s)}$$
$$\geqslant m(m-1)(\sigma_r(2s, n, m))^{(2s+1)/(2s)}.$$

[6] These two relations can be regarded as bounds for m, given s. For example, for $s = 1$ one needs $m > \frac{1}{2}((4(n-1)^3 - 3(n-1)^2)^{1/2} + 3(n-1))$.

Combining this inequality with (19), in which we put $t = 2s + 1$, we find that

$$2\sum_{i=1}^{m_1} \xi_i^{2s+1} \geqslant m(m-1)\,\Phi_r(s, n, m).$$

Hence, in view of the theorem's hypothesis that $\Phi_r(s, n, m) > 0$, it follows that the sum on the left side of the last relation contains at least one summand. Therefore

$$\gamma(\mathfrak{A}(K)) = \max_{1\leqslant i\leqslant m_1} \xi_i\,, \qquad (\gamma(\mathfrak{A}(K)))^{2s+1} \geqslant \tfrac{1}{2}\Phi_r(s, n, m),$$

which proves the theorem.

Writing out the estimate which follows from Theorem 1 when $s = 1$, $m = (n-1)^2$, we obtain

$$d_r(n, (n-1)^2) \leqslant \frac{2(n-r)r}{n}\left(1 - \left(\frac{1}{2}\left(n^{-3/2} + \frac{n^2 - 4r(n-r)}{r(n-r)\,n(n-1)(n-2)^2} - \frac{1}{n(n-2)}\right)\right)^{1/3}\right).$$

THEOREM 2. *Let r and d be integer-valued functions of n such that for $n \to \infty$, $r/n \to \rho$, $0 < \rho \leqslant 1/2$, $d/n \to \delta$, $0 < \delta \leqslant 2g$, where $g = \rho(1-\rho)$. Then* (2) *holds.*

Proof. Let s be an integer-valued function of n such that $2s/n \to \gamma$, $\gamma > 0$, $n \to \infty$. We shall show that

$$n^{-1} \ln R_{2s}(n, r) \sim \max_{0\leqslant\theta\leqslant g} \varphi(\gamma, \theta), \qquad n \to \infty, \tag{20}$$

where $\phi(\gamma, \theta) = -H(\rho) + \gamma \ln(1 - \theta g^{-1}) + \rho H(\theta/\rho) + (1-\rho)\,H(\theta/(1-\rho))$ and $R_{2s}(n, r)$ is defined by (14).

In fact, it is obvious that $n^{-1} \ln R_{2s}(n, r) \sim \max_{0\leqslant\theta\leqslant\rho} \phi_1(\gamma, \theta)$, where $\phi_1(\gamma, \theta) = -H(\rho) + \gamma \ln|1 - \theta g^{-1}| + \rho H(\theta/\rho) + (1-\rho)\,H(\theta/(1-\rho))$ is the asymptotic approximation to the logarithms of the summands of $R_{2s}(n, r)$. Let θ' be a point of the interval $(g, \rho]$ and let $-\beta = 1 - \theta' g^{-1}$ ($\beta > 0$). Let us define θ by $1 - \theta g^{-1} = \beta$. Clearly $\theta = g(1-\beta)$, $\theta \in [0, g)$, and $\theta' = g(1+\beta)$. As is easy to verify, the derivative with respect to β of $f(\beta) = \phi_1(\gamma, g(1-\beta)) - \phi_1(\gamma, g(1+\beta))$ is nonnegative for $0 \leqslant \beta \leqslant \rho/(1-\rho)$ and $f(0) = 0$, and hence $\phi_1(\gamma, \theta) \geqslant \phi_1(\gamma, \theta')$. This proves the desired result, since $\theta \in [0, g)$, while $\theta' \in (g, \rho]$.

For further presentation it is convenient to assume that γ is the following function of an independent parameter α, $0 < \alpha \leqslant g$:

$$\gamma(\alpha) = (g - \alpha) \ln((g - \alpha + \alpha^2)/\alpha^2). \tag{21}$$

(The function $\gamma(\alpha)$ transforms the interval $(0, g]$ one-to-one onto the positive half-axis.) Relation (21) was chosen so that $\partial\phi(\gamma(\alpha), \theta)/\partial\theta$ becomes 0 at the point $\theta = \alpha$. It follows from this that the maximum in (2) equals $\phi(\gamma(\alpha), \alpha)$.

Set $m(s) = [nR_{2s}^{-1}(n, r)]$, where $[x]$ is the integer part of x. We will show that

$$(2s)^{-1} \ln \Phi_r(s, n, m(s)) \sim \varphi(\gamma(\alpha), \alpha)/\gamma(\alpha)), \qquad n \to \infty. \tag{22}$$

As a preliminary, let us note that from (20) and the definition of $\gamma(\alpha)$ it follows that

$$(R_{2s}(n, r))^{1/2s} \sim \exp(\varphi(\gamma(\alpha), \alpha)/\gamma(\alpha)), \qquad n \to \infty. \tag{23}$$

From the definition of $\Phi_r(s, n, m)$ we obtain

$$\Phi_r(s, n, m(s)) \sim \tfrac{1}{2}(R_{2s}(n, r)(1 - 1/n))^{(2s+1)/(2s)} + R_{2s+1}(n, r) - n^{-1}R_{2s}(n, r), \qquad n \to \infty.$$

Now (22) follows from the above, the relation $R_{2s+1}(n, r) \geqslant 0$ (Corollary 2) and (23).

Let us put $m = m(s)$ in Theorem 1. With the help of (22) we obtain the following bound for α:

$$\delta/2 \lesssim g(1 - \exp(\varphi(\gamma(\alpha), \alpha)/\gamma(\alpha)) = \psi(\alpha), \qquad n \to \infty, \tag{24}$$

where $\psi(\alpha)$ is an increasing function[7] of α†. On the other hand, α is defined uniquely by $-\phi(\gamma(\alpha), \alpha) = \lim_{n\to\infty} n^{-1} \ln m(s)$, where $-\phi(\gamma(\alpha), \alpha)$ is a decreasing function[8] of α. Hence it follows that if α' is the minimal α for which (24) is satisfied (i.e., α' is the root of (3)), then

$$n^{-1} \ln m_r(n, d) \lesssim -\varphi(\gamma(\alpha'), \alpha'), \qquad n \to \infty.$$

This bound coincides with (2), since $-\phi(\gamma(\alpha), \alpha) = \gamma(\alpha) \cdot \ln(1 - \delta(2g)^{-1})$. This proves the theorem.

Let us compare the above bound for $m_r(n, d)$ with the results of Levenshtein (1971). Expanding the right side of (2) in powers of $1 - \delta(2g)^{-1} = x_0$, we obtain, for $1/4 \geqslant g \geqslant \delta/2$,

$$n^{-1} \ln m_r(n, d) \lesssim -e(x_0)^2 \ln(x_0) + O((x_0) \ln(x_0)), \qquad n \to \infty. \tag{25}$$

[7] Since $d\psi(\alpha)/d\alpha \geqslant 0$, $\alpha \geqslant 0$.

† Translator's note: The original paper states incorrectly that $\psi(\alpha)$ is a decreasing and $-\phi(\gamma(\alpha), \alpha)$ an increasing function.

[8] Since its derivative is negative for $\alpha > 0$.

The bound for $m_r(n, d)$, which was obtained in Sidelnikov (1971), we will write in the form

$$n^{-1} \ln m_r(n, d) \lesssim H(\rho) - H(\rho_0), \qquad n \to \infty, \tag{26}$$

where $1/4 \geqslant g \geqslant \delta/2$ and $\rho_0 = 1/2 - (1 - 2\delta)^{1/2}/2$ (the smaller root of the equation $\rho(1 - \rho) = \delta/2$). For ρ close to ρ_0 the right side of (26) can clearly be represented in the form

$$H(\rho) - H(\rho_0) = \frac{g}{(1 - \rho - \rho_0)} \left(1 - \frac{\delta}{2g}\right) \ln \frac{1 + (1 - 2\delta)^{1/2}}{1 - (1 - 2\delta)^{1/2}} + O\left(\left(1 - \frac{\delta}{2g}\right)^2\right). \tag{27}$$

Comparison of (25) and (27) shows that for δ lying in an interval (δ_0, g), $g \leqslant 1/4$, where δ_0 ($\delta_0 < 2g$) is a certain constant depending on g, the bound (2) is better than (26).

Let us note that from the estimate (2) together with (12) of Levenshtein (1971) there follows an estimate better than (26) for all δ, $0 < \delta < 2g$.

3. Bounds for the Cardinality of a Binary Code

Theorem 3. *Let $d(n)$ be an integer-valued function of n such that $\lim_{n\to\infty} d/n = \delta$, $0 < \delta \leqslant 1/2$. Then*

$$n^{-1} \ln m(n, d) \lesssim \ln 2 - \max_{\delta/2 \leqslant g \leqslant 1/4} G(g, \alpha), \qquad n \to \infty, \tag{28}$$

where $G(g, \alpha) = H(\rho) - (\alpha - g) \ln((g - \alpha + \alpha^2)/\alpha^2) \ln(1 - \delta(2g)^{-1})$, $g = \rho(1 - \rho)$ and $\alpha = \alpha(\rho)$ is the root of (3).

The proof follows immediately from (5) and (2).

Let us show that (28) can be written in the form (1). In fact, it follows from (25) that in a neighborhood of the point $g = \delta/2$, $g \geqslant \delta/2$ the function $G(g, \alpha)$ can be expressed in the form

$$G(g, \alpha) = H(\rho) + e(1 - \delta(2g)^{-1})^2 \ln(1 - \delta(2g)^{-1}) + o((1 - \delta(2g)^{-1})^2).$$

Since the derivative $dH(\rho)/dg$ is positive at the point $g = \delta/2$, $\delta < 1/2$, we conclude that $\max_{\delta/2 \leqslant g \leqslant 1/4} G(g, \alpha) = H(\rho_0) + \epsilon(\delta)$, where $\epsilon(\delta) > 0$ for $0 < \delta < 1/2$ and $\rho_0 = 1/2 - (1 - 2\delta)^{1/2}/2$ (the smaller root of $\rho(1 - \rho) = \delta/2$).

Obviously the right side of (28) equals $\ln 2 - G(g_0, \alpha_0)$, where (g_0, α_0) is a solution to the system of equations consisting of (3) and the equation $dG(g, \alpha)/dg = 0$.[9]

The author has often discussed with V. I. Levenshtein the problems and results described in this paper, and in fact his advice was helpful in obtaining the bound (15). The author expresses his gratitude to V. I. Levenshstein for this.

RECEIVED: December 1974

REFERENCES

BASSALYGO, L. A. (1965), New upper bounds for error-correcting codes (in Russian) *Probl. Peredachi Inform.* **1**, 4, 41–44.

BERLEKAMP, E. R. (1971), "Algebraic Coding Theory" (Russian translation), Mir, Moscow.

HARDY, G. H., LITTLEWOOD, J. E., AND POLYA, G. (1948), "Inequalities" (Russian translation), Moscow.

LEVENSHTEIN, V. I. (1971), On upper bounds for codes with codewords of a fixed weight (in Russian) *Probl. Peredachi Inform.* **7**, 4, 3–12.

SIDELNIKOV, V. M. (in press), New bounds for the density of sphere packings in an n-dimensional Euclidean space.

SIDELNIKOV, V. M. (1973), On the density of sphere packings on the surface of an n-dimensional Euclidean sphere and on the cardinality of a binary code with a given minimum distance (in Russian) *Dokl. Akad. Nauk SSSR* **213**, 5, 1029–1032.

SIDELNIKOV, V. M. (1971), On the auto-correlation of sequences (in Russian) *Probl. Kibern.* **24**, 15–42.

[9] This equation may be written out explicitly, but the resulting expansion is too unwieldy.